Summary: The paper refines known estimates of time and memory complexities of Oorschot and Wiener algorithm for the “gold” collision searching. We use results related to the computation of characteristics of time-memory-data tradeoff method with distinguished points. Probabilistic approximations of the algorithm characteristics by random variables depending on the number of particles and the total number of particles in a subcritical Galton-Watson process are described. The limits of expectations of these random variables are found.

MSC:

68W40 Analysis of algorithms
94A60 Cryptography

Keywords:
gold collision search; time-memory-data tradeoff with distinguished points; branching processes; one-way function inversion

Full Text: DOI MNR

References:


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.